STRATEGY RESEARCH PROJECT

INFORMATION WARFARE
IS IT FEASIBLE? DESIRABLE?

BY

LIEUTENANT COLONEL THOMAS E. WARD II
United States Army

USAWC CLASS OF 1996

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

LIST OF FIGURES

ABSTRACT

AUTHOR: Thomas E. Ward, II (LTC) USA

TITLE: Information Warfare: Is It Feasible? Desirable?

FORMAT: Strategy Research Project

DATE: 29 March 1996 PAGES: 28 CLASSIFICATION: Unclassified

Information Warfare is a hot topic throughout the Department of Defense today, and a debate rages about what it really is, who the warfighters are, and what its impact will be on warfare in the future. This study defines key concepts of information warfare, examines its offensive and defensive components, and compares information warfare to a previous technological revolution, air warfare. The paper draws on a broad spectrum of resources from military, philosophy, business, and computer-oriented perspectives. It examines opportunities and potential pitfalls in the conduct of offensive and defensive information warfare, the desirability and feasibility of using information warfare weapons and techniques, and concludes with precautionary caveats about vulnerabilities, expectations, and applicability.

WHAT IS THE INFORMATION WAR?

Introduction

"We must, above all, win the information war!"[1] These words have become a battle cry for the U. S. Army. General Gordon Sullivan brought the phrase into the Army's lexicon, and a change of Army leadership has only intensified what General Sullivan started. His successor as Chief of Staff, General Dennis Reimer, lists "win the information war" as one of his top priorities as well. The message is clear: a key to future victory is digitizing the battlefield, and we see enormous effort and resources applied to Force XXI and the Experimental Force (EXFOR).[2] Information warfare is a hot topic, and not only in the US Army. Other services are following parallel paths, and if anything are even more enthusiastic and determined. Predictably, each service has its own ideas about service contributions to the Information War. Information warfare (IW) is now listed as part of the 1995 National Military Strategy, in the "Fight and Win" column.[3] This is serious business, and it will certainly be JOINT business. But is information warfare really feasible? What about the desirability of IW? Is it more desirable than traditional physical combat? In this paper, we will see that IW is not only feasible, it has become an integral part of modern warfare. We will answer

the question of desirability as well, and identify some important caveats that qualify the conclusion.

Background

Futurists tell us we are entering the "third wave." The agrarian era is behind us, and we are witnessing the transition from an industrial age to an information age. We stand on the threshold of an era when information is the product, and information itself constitutes both wealth and power.[4] If information is power, or the possession of information confers power, it follows logically that this power might also be used as a weapon, just as the power of gunpowder and the internal combustion engine were harnessed, and became powerful weapons of warfare.[5]

Then again, neither gunpowder nor the internal combustion engine were weapons of war in and of themselves. To be sure, they were key technology breakthroughs in the development of the modern machines of war. These machines gave their owners tactical, operational, and strategic advantages against their enemies. But to contribute to the battle, these technological marvels had to be weaponized, aimed, and operated with great skill. Despite repeated predictions to the contrary, no technological innovation has replaced the *warrior*. Technology has often changed the arms and armor, and even the medium of battle. The fighter pilot in his sleek, high-tech war machine is a far cry from the grunt in a foxhole, but he is no less a warrior, and few would argue that *both* are still absolutely indispensable on the modern

battlefield. Will the information war change these facts, or will it simply alter the equation?

First, however a short discussion of "information" is in order. Understanding and agreeing upon a hierarchy of data, information, and knowledge will help clarify the discussion. Information, in and of itself, is worthless. Information only becomes valuable when it increases knowledge, and that knowledge is used with wisdom. Figure 1 provides an illustration of the hierarchy of information.[6] Data provided by a variety of sensors is the lowest form, and must be collected to reveal patterns of discernable information. The information is analyzed to produce knowledge of an

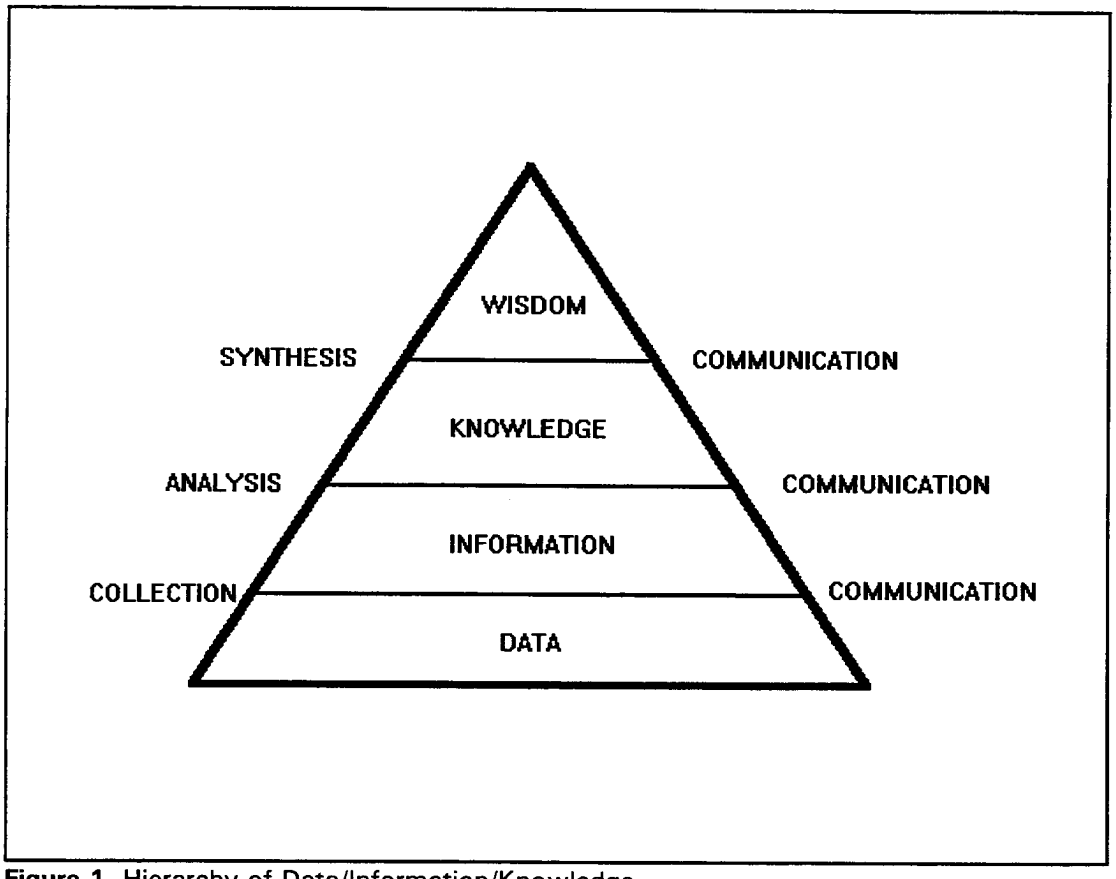

Figure 1 Hierarchy of Data/Information/Knowledge

event, area, or situation. Finally, synthesis of knowledge should produce wisdom, the appropriate use of knowledge in action. Despite the value added at each level of the hierarchy, knowledge is valueless unless it is used with wisdom. Notice also that communication is the "mortar" holding this pyramid together. In virtually every discussion of Information Warfare, regardless of means, the goal is twofold and complementary: 1) increase the situational awareness of friendly forces (especially leaders), and 2) disrupt or destroy the situational awareness of the enemy.

Definitions

If we are to discuss this subject, it is essential to first agree on a common set of definitions. At the moment, many doctrinal publications are still in draft or review form. We haven't quite reached a consensus about what the information war really is. For the purposes of this paper, at least, the following definitions are critical.

What is the Information War?

In every case, the common thread running through the description of efforts in the information war is an effort to increase or decrease the situational awareness of someone, usually a key decision maker.[7] Typically, the commander is the focus of attention, but we have begun to realize that information is also valuable when it is sent down as well as up, and that lateral transmission of information on the battlefield can increases effectiveness of both "shooters" and those who support or supply the shooters. Digital technology is the vehicle that is allowing great strides to be made,

replacing voice communication with digital, using electronically generated symbology, increasing both the speed of transmission, and the level of understanding upon receipt. We can say, from a military perspective at least, that the information war is an effort to increase or decrease the situational awareness of warriors on the battlefield, wherever that battlefield may be.

So What Is Information Warfare?

Information warfare consists of "actions taken to achieve information superiority by affecting adversary information, information-based processes, and information systems while defending one's own information, information-based processes, and information systems."[8] This definition brings to light an often-overlooked but critical factor in discussions of IW: it consists of both offensive and defensive components. Offensive information warfare (OIW) seeks to disrupt or deny the enemy the use of his systems. A subset of OIW is Command and Control Warfare (C2W), in which the object of operations is specifically to disrupt or deny an adversary's ability to exercise command and control of his forces.[9] On the other hand, defensive information warfare (DIW) seeks to preserve our ability to use our own information systems. Furthermore, IW operations may be closely related to Intelligence and Electronic Warfare (IEW) operations, but the terms are not interchangeable, in either the offensive (EW) or defensive (intelligence/ counterintelligence) context. This is a critical conceptual hurdle. IW may be a component of IEW, or vice versa, but the two are not synonymous.[10] We will discuss

the characteristics of offensive and defensive IW operations in greater detail later in this paper.

Cyberwar and Netwar

In a recent project for RAND, John Arquilla and David Ronfeldt present two new words for the lexicon: cyberwar and netwar.[11] According to Arquilla and Ronfeldt, *cyberwar* is a component of "conventional" military contests; that part of the conflict oriented toward collection, analysis, communication, and use of knowledge. Information technology is a component of cyberwar in that it makes distribution of information possible, but the second order effect of "networking" is at least as significant. Arquilla and Ronfeldt propose that the hierarchical structures of military systems will be much less exclusive than today, that networks will often replace hierarchies in conflict. The information revolution is making this possible by permitting horizontal distribution of information, a key element of networks. With possession of the information, and its accompanying knowledge, relatively autonomous portions of the network will be able to do the right thing, not only responding to situations, but anticipating, and acting proactively, without orders from above. At the same time, because of the rapid transmission of information up the chain of command, leaders will enjoy greater oversight of events.

On the other hand, *netwar* has much less to do with exploitation or destruction of C3I systems, than it does with the second and third order effects of the information revolution. Again, electronic networking is a key component. The important

distinction between netwar and cyberwar, in the definitions provided by Arquilla and Ronfeldt, is that *cyberwar is part of a military operation with "conventional" forces and battles, while netwar is information warfare without military forces or physical battles.*[12]

Information Dominance

Information dominance is the ultimate objective of "the information war." The purpose of IW, whether it is cyberwar in conjunction with conventional forces, or netwar without traditional battle is to thin or disperse the fog of war for us and our allies, while thickening that shroud of fog around our enemies. Neither OIW nor DIW need to be perfect or absolute. The goal is to widen the knowledge gap between friendly and enemy forces - and the wider the better. The side that knows more will have a decided advantage over its adversary, as long as it is able to use that knowledge.

OFFENSIVE AND DEFENSIVE INFORMATION WARFARE

Information Warfare has two distinct thrusts: how to inflict maximum damage on an adversary, and how to prevent being the victim of IW attack. What opportunities and pitfalls does IW promise, and how does the commander fit IW into his offensive and defensive plans?

Offensive Information Warfare

This is the area where we have seen the most speculation so far, and the greatest promise for maximum gain at minimum cost - the war in cyberspace - "Let's cripple the enemy before he has an opportunity to fire a shot." Many have said that the Persian Gulf War was the first modern information war.[13] It certainly provides an excellent example of an offensive C2W battle as an integral, essential component of the overall campaign plan. For example, one of the new weapons first tested in combat was a warhead for the Tomahawk cruise missile that fed out carbon fiber filaments as it flew over electrical distribution facilities to short them out, subsequently crippling the Iraqi air defense system.[14] The central telephone exchange in Baghdad was among the first targets engaged in the air campaign. But even before

the telephone exchange was attacked, anti-aircraft radars were targeted and eliminated by Army Apache helicopters.[15] Each of these events was part of the integrated plan to sever the "head" of the Iraqi military machine from its "arms"- disrupt or destroy the system of command and control. The goal was to blind or destroy the sensors, eliminating the acquisition of information; and disrupt or destroy the communications system, preventing the transmission of information upward or control orders downward. The opening shots, indeed major portions of the air campaign, were designed to deny the Iraqis the ability to gather information or to communicate information. The virtual elimination of the Iraqi Air Force was absolutely critical, in blinding the intelligence-gathering capability that could have spoiled the element of surprise necessary to pull off the "left hook" flanking maneuver that General Schwarzkopf referred to as his "Hail Mary." This was all information warfare, but it was also very violent and physically destructive, a far cry from "netwar" or the "bloodless war of cyberspace."

Immediately after the Persian Gulf conflict, reports of cyberwar directed against the Iraqis began to appear. Open-source periodicals reported that a computer virus was injected into the Iraqi anti-aircraft command and control system through a computer printer that was delivered sometime between the invasion and liberation of Kuwait. According to the report, command and control of Iraqi anti-aircraft systems was virtually eliminated by the virus, before the coalition air campaign began. In retrospect, the report appears to be a hoax.[16] Just the same, it highlights a serious problem with IW in support of combat operations. How do you assess battle damage?

Theoretically, if you can functionally destroy or sufficiently disrupt command, control, and communications, physical destruction of C3 assets will be unnecessary. Furthermore, if you can sever the head from the arms by isolating the leadership from its armed forces, you may obviate the need to engage the enemy's armed forces in "real" combat at all. Still, the task of assessing battle damage as a result of offensive cyberwar attack is a real problem, which will be examined more closely in the section covering opportunities and pitfalls.

At the tactical and operational level, we already possess tools to conduct effective offensive IW. Perhaps surprisingly, most IW tools available at the tactical and operational level are sophisticated and effective, but still relatively conventional. For example, cruise missiles or laser guided bombs delivered by stealth aircraft are tremendous IW weapons. What makes them IW weapons is the selection of the target. The thrust of offensive IW at these levels of warfare is also a relatively conventional objective: increase the fog of war for the enemy.

What about cyberwar? Is there a place for cyberwar at the tactical and operational level? Absolutely, but two factors stand out. First, while the execution of any operation is a tactical event, the decision to inject or activate disabling software code or remotely manipulate data is likely to be made at the national level, and accomplished with strategic assets. Second, because the effects of cyberwar are so difficult to assess, targets will most likely be struck with "hard kill" weapons as well, to provide a comfortable assurance of target destruction. If destruction of those targets is made less costly by the "cyberwar prep," the IW efforts were well spent.

Does this mean that IW can be waged with both conventional and unconventional weapons? It certainly does. IW can be waged by targeting conventional weapons at informational targets, by launching cyberweapons such as disabling code at a variety of informational targets, or by a combination of the two. In the future, we should expect to see the combination emerge as a preferred solution, to capitalize on the synergy of the two techniques.

Defensive Information Warfare

If there is an area suffering from benign neglect, this is it. Defensive operations have never enjoyed the glamour, the esprit, the appeal of offensive operations, and the same attitude is equally applicable to information operations. Today, at least within the U.S. military, even defensive operations are described in terms formerly used only for offensive operations, and defense is often seen as an unpleasant necessity, rather then "real" warfare.[17] Philosophically, it is easy to lose sight of the fact that successful defense is absolutely essential to victory in any conflict. True, defensive operations alone will not win a war. We take it as an obvious truth that defensive operations are to be followed at the soonest possible moment by offensive operations, leading to termination of hostilities under conditions favorable to the United States. At the same time, the United States takes pride in maintaining that it is not an aggressor nation, that it does not start wars. This position almost guarantees that in virtually any conflict, United States forces will begin from a defensive posture, until sufficient combat power is built up to launch offensive

operations. While it may be true that even the most successful defense is unlikely to win a conflict, it is also just as true that an unsuccessful defense can make subsequent operations of any sort difficult, if not impossible.

The same principles are true in information warfare. Successful defensive information warfare is essential to both offensive and defensive combat operations. With the increasing value of information as a commodity, protection of our own information resources and denial of those same resources to an adversary are essential. We are still faced with the "glamour problem" - it is much more exciting to inflict damage on another than to prevent damage to ourselves. The hackers get the headlines, but instances of successful defense of data resources are considered "non-news." Regardless, what are the specific objectives of defensive information warfare and how can we achieve them? Here are three key components:

1. Protect the Friendly Information Architecture From Damage/Destruction

Obviously, we want to be able to use our own information system for the millions of tasks and transactions it supports, from ordering replacement parts for combat vehicles, to storing and communicating operational plans, to paying the forces in the field. We have come to rely on our information systems to increase efficiency, operational tempo and lethality, to offset the reductions in sheer numbers of forces. We have chosen to maintain a qualitative edge over adversaries, rather than a quantitative superiority. That qualitative edge is largely dependent on the ability to process information at a pace that was previously considered impossible. While the

individual bits of hardware are often the focus of attention, defending the mortar that glues the structure together is the key to success. (Refer once again to Figure 1, on page 3.) To acquire value, information must not only be collected, it must be communicated. Consequently, to protect our information architecture, we must not only physically protect the processors from damage or corruption, we must protect the means of communication as well. An interesting dilemma is developing in the area of communications. Increasingly, U.S. military forces are relying on commercially available communications systems. This is a good news/bad news story. Lease or purchase of commercial communications provides capacity at relatively low cost. At the same time, however, it also introduces new vulnerabilities. First, these same links are available to anyone with the money to purchase the services. Furthermore, they do not enjoy the same sort of "hardening" typical of tactical military systems. Today, 90% of DOD communications are transmitted over commercial systems.[18]

2. Deny Enemy Intrusion and Access/Theft/Corruption.

We might enjoy the advantage of a truly phenomenal information collection and distribution system, but if our system is an open book to an adversary, the relative value evaporates. "Information dominance" is the key term here. Our systems must be secure from intrusion that would allow reading, altering, or destroying information we possess. This is not simply a battlefield problem. There is also an even more basic, fundamental level of defense - a pressing need for information to be secure at its source. For example, what value is a replacement part for an aircraft if a design

flaw was surreptitiously inserted into the technical data package, that would virtually insure catastrophic failure within ten hours of operation? Very quickly, we see that defensive information operations are a challenge that reach all the way back to the industrial base, not just the combat forces in the field.

3. Deny enemy knowledge by passive means

Passive defense is the least glamorous task of all, yet it may also be the most effective. Simply stated, we must ensure we do not broadcast information to an adversary, or allow him to gather worthwhile information by observation. Adherence to rules for handling classified information, and good operations security (OPSEC) will prevent adversary collection of information "the easy way."

Relevance to the Commander

The important concept to recognize is that information warfare consists of both offensive and defensive aspects. While we certainly want to pursue the capability to wage offensive information operations, we must keep part of our attention focused on the defensive portion as well. The potential advantages to be gained through the use of OIW are matched and even exceeded by unsuccessful DIW. While high tech intrusions get the headlines, the highest payoff in DIW still comes from attention to detail in following familiar physical security and information security procedures, and old-fashioned OPSEC.[19,20]

A LESSON FROM HISTORY:

THE UNFULFILLED PROMISE OF STRATEGIC BOMBING

Since the invention of the airplane, proponents of airpower have maintained that the airplane has fundamentally changed the nature of war.[21] If we examine this claim dispassionately, we see that it has some elements of truth, and some unfulfilled promises as well. For example, while dominance in the aerial dimension of warfare is an essential for success on the surface, employment of air forces has not eliminated the function of surface forces on land or at sea. The greatest successes in modern combat have been achieved by the integration of air, sea, and land forces, capitalizing on the synergy of the combination. Those who have advocated "winning the war" with strategic bombing alone have invariably been disappointed, or forced to present specious arguments after the fact, that they weren't given enough time, or freedom to hit appropriate targets.[22] Even the rapid capitulation of Japan following the atomic bombing of Hiroshima and Nagasaki is suspect. How much was Japan's surrender due to its loss of natural resources from the submarine campaign, or from the combined-services island hopping campaigns across the Pacific, as well as the strategic bombing campaign? Unquestionably the shock to the Japanese as they faced the realities of Hiroshima and Nagasaki was profound.[23] Yet today, many historians agree that it was

the combination of factors, and the inevitability of their combined outcomes, not the atomic bombs alone, that prompted Japan's surrender.[24] Hiroshima and Nagasaki were the straws that broke the back of the Japanese camel (big, heavy straws though they were).

The events of history since then have only strengthened the argument. Conflicts in Korea, Vietnam, and even Desert Storm demonstrated that air power was essential for success on the battlefield, but that airpower alone did not bring conflicts to a satisfactory conclusion. Airpower can set the stage for overwhelming success on the battlefield, yet many of the "centers of gravity" chosen for strategic bombing have proven elusive, if not impossible to effectively target. The most elusive of all strategic targets has been the will of the political leadership, and of the people to wage war. Again, history has indicated that "strategic" aerial bombardment campaigns against large, predominantly civilian targets may fail to destroy the resolve of its intended victims.[25] The citizens of Great Britain, Germany, Vietnam, and of Baghdad all provide testimony to this fact. Humans who are fighting together for a common cause are amazingly resilient, and willing to undergo incredible hardship. Typically, they are strangely, even perversely bonded when confronted with a common enemy, even one from the skies. They may become effectively helpless and defenseless, but they are seldom, if ever, less defiant. Even Japan was ultimately occupied to accomplish control over its population.[26] Airpower makes stunning victory possible, but it does not achieve victory alone.

Today, we find proponents of offensive IW espousing theories similar to those of strategic bombing proponents. "We can win the war without bloodshed" is a common theme. We should approach these claims with skeptical caution. A common "nightmare scenario" in popular fiction today is the corruption or destruction of the New York Stock Exchange information systems,[27] or collapsing the banking system by bringing down a major bank.[28] Either of these events would seriously damage the United States, but would they bring about its capitulation in a dispute over a vital national interest? Probably not. There is a tendency among some to assume that humans cannot survive without luxuries once they have become accustomed to them. But in what historical example has this ever been true?

Information warfare will be a key component of future conflicts, just as the battle for air superiority has become a key component. Both offensive and defensive aspects will be essential for success. Successful DIW will allow combat forces to operate without crippling disruption, and successful OIW will allow them to enjoy the benefits of information dominance: to see the battle space clearly, while enshrouding the enemy in fog. However, neither vision nor fog win or lose battles alone. Victory in any form comes from the innovative, effective application of combat power. Just as airpower has become an indispensable part of combat power, so information warfare is becoming an integral part of warfare in general. We are expecting far too much, however, if we expect IW to become the only effective means of warfare.

OPPORTUNITIES AND POTENTIAL PITFALLS

Information Warfare Across the Spectrum of Conflict

A unique aspect of OIW is that it can be either passive (non-invasive) or active (invasive). The distinction is important. Interception of electromagnetic radiation is a passive activity. There may be a great deal of effort involved, but it is non-invasive. In the United States we call it intelligence gathering, by National Technical Means. Penetration of a computer or computer network, on the other hand, is invasive, even if the purpose, once penetration is accomplished, is merely to look and listen. The next step, either corruption and manipulation of data, or denial of service is not only active, it is destructive and provocative. Consider Figure 2. Across the spectrum of conflict there is a risk to payoff ratio that should be considered. During peacetime, the provocative nature of disruptive OIW may be perceived as risky. As the level of conflict escalates, the risk to benefit ratio rises, and OIW can increasingly be used as a tool of competition. Indeed, its greatest value may be during political/economic competition and transition to war. But this increasing value holds true only up to a point. Effective OIW may be employed in lieu of armed conflict, or as an adjunct supporting other activities as the level of conflict rises. There is a point of diminishing returns, however, as the level of conflict escalates, until OIW becomes an

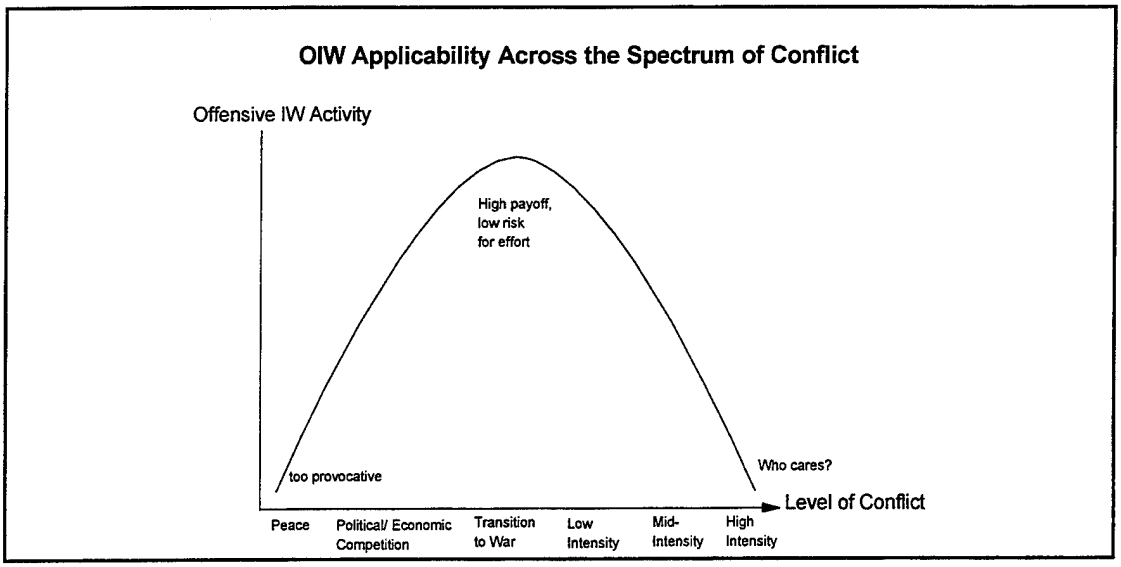

Figure 2 OIW Applicability and Risk/ Benefit Relationships

insignificant factor in comparison to the physical damage accomplished. It becomes a tricky, and unpredictable calculus. Could IW assume the role of anti-war, averting armed conflict, as the Tofflers contend?[29] Or would invasive OIW prove to be a prod that pushes belligerents from peaceful competition to open, armed conflict? Opinions vary. George J. Stein argues that the unpredictable effects of IW gravitate against its use, at least by nation-states.[30]

Operations Other Than War

Information Warfare, in the form of a purely electronic cyberwar or netwar, provides the potential for conducting operations against an adversary that may significantly degrade his warmaking potential. These operations are most likely to be covert, may be undetectable to an adversary, and be impossible to attribute to an opponent even if they are detected. Are these military operations, are they

intelligence operations, or are they something else? The answer is neither simple or straightforward, for IW is in fact all three.

What is the potential for IW as an OOTW when employed to support the national interest? The potential is great indeed. Effective OIW operations could permit the U.S. to predict, with near certainty, the operations of an adversary. Furthermore, OIW could seriously disable the combat capabilities of an adversary by disrupting C4I (command, control, communication, computers, and intelligence) from top to bottom. Preemptive OIW might convince an enemy to forego dangerous, risky behavior, by destroying his confidence in his own systems and forces.

What is the potential for damage to the national interests if directed against the United States? Here we face a true dilemma, for the greater we leverage our own combat capabilities through digitization and telecommunication, the more we are dependent on those systems. Consequently, we create vulnerabilities if those systems can be attacked. The need for robust communications becomes obvious. If not sufficiently robust redundant, telecommunications could easily become the Achilles Heel of U.S. forces.[31]

What would be an appropriate response to an IW attack on interests vital to the U.S.? Certainly a response in kind would be both appropriate and convenient, but do nation-states such as Libya or Iran have similar vulnerabilities? We should not limit ourselves to response in kind, but consider physical attack of both counterforce (military) and countervalue (civilian infrastructure) targets to quickly convince aggressors that such adventurism is unprofitable.

Does IW Offer Opportunities for Asymmetrical Battle?

Absolutely. The ideal situation for any commander is to own a monopoly on an effective weapon against which an adversary has little or no defense. History provides several examples: the tank, the submarine, the atomic bomb, the sea-skimming and cruise missiles. Is information warfare such a weapon? From the vantage point of today, we must conclude that it is. A belligerent that cannot trust its knowledge of an enemy or of itself is virtually helpless. The Persian Gulf War provides convincing evidence. Coalition forces used sea-, air-, land-, and space-based platforms to collect information about the Iraqis, then methodically, violently disrupted and destroyed the C2 capability of the Iraqi war machine.[32] Once that had been accomplished, the destruction of the forces themselves proved to be relatively easy and inexpensive. This was an example of one of the facets of asymmetric battle. It was a case of "high tech" versus "medium tech," and high tech was the clear victor. Colonel Edward Mann's words describe the situation perfectly: "Saddam Hussein's industrial-era armed forces ran up against a post-industrial whirlwind."[33] It is ironic, yet predictable, that the most disturbing weapon used by the Iraqis was the surface to surface ballistic missile, against which we had little effective counter. The Iraqis' only success was this asymmetric attack.

History also tells us that monopolies are fleeting. Does the U.S. have an effective monopoly, and if so, how long will the monopoly last? In its ability to physically reach out and destroy critical C2 facilities, the U.S. currently has no peer. In warfare, as in business, one must never rely on a monopoly alone for success,

because monopolistic conditions do not prevail indefinitely. Furthermore, response in kind may not be the response to fear. Any adversary of the U.S. would have to consider very carefully its objectives in opposing the U.S. Could it use IW to sufficiently impair U.S. response capability, so that its limited objectives were simply not worth the trouble to oppose? The possibilities could be tempting. It is clear from Iraq's experience that direct military confrontation of the U.S. is an uninviting prospect. How might an adversary use IW to pursue asymmetric attack of US vulnerabilities in pursuit of limited objectives? Two opportunities for strategic and operational-level "IW fire and maneuver" attack against the United States seem fairly clear. First, disrupt US communications, as discussed in "Operations Other Than War" previously. Second, disrupt the ability of US forces to deploy. The two are closely inter-related. The huge, complex process of deployment is dependent on commercial communication and transportation systems that are relatively "soft" targets. Disruption of commercial communication systems and the transportation infrastructure supporting deployment would present an inviting target.

Who Is Most Vulnerable?

Without an effective defense, the degree of vulnerability to IW attack is directly proportional to the leverage gained by use of information as an asset. If information technology has increased a belligerent's capability by an order of magnitude, then successful attack of that technological capability can degrade by an order of magnitude. This kind of math can either tilt or level a playing field very

quickly. At present, the US leads the pack. It has been the most successful at employing IW in support of conventional warfare. But has it had to defend against determined IW attack? Apparently not, at least not since the Vietnam war.[34] Adversaries have either failed to recognize vulnerabilities, or have been unable to attack them. Still, unless the systems that create information dominance are successfully defended, they present a dangerous vulnerability.

Once again, there is an opposite side of this coin. One IRA bombing attack on the financial district in London resulted in damages of $1 billion, much of it in lost business, rather than physical damage. This is an excellent example of low tech applying high leverage on a high tech system with an asymmetrical attack.[35]

An End to Bloodshed?

Is information warfare likely to become a replacement for the bloody combat man has known throughout his existence? Not entirely, but perhaps in a small way. Here is where the distinction between cyberwar and netwar is significant. Remember, *cyberwar*, as defined by Arquilla and Ronfeldt, is part of a military operation with conventional forces and battles, while *netwar* is IW without military forces or battles. The IW conflict may become primarily a "guerilla" war that seldom, if ever, achieves nation versus nation emphasis. Nation-states may be reluctant to use this weapon in lieu of conflict because of the likelihood of "real" (physical) retaliation, at least if they believe their actions can be traced.[36] That leaves the actors who are not nation-states as likely aggressors, at least in the "war without bloodshed," or netwar. The

possibility of netwar as cyber-terrorism is genuine. The technique has real advantages, as a successful attack could be extremely disruptive, demonstrating the powerlessness of a government, while avoiding the negative backlash that results from apparently ruthless killing. Additionally, IW (cyberwar) is likely to be conducted as a prelude to war, to set favorable preconditions for conflict.

IW could be perceived as an attractive alternative to conventional warfare. Just the same, we cannot escape the conclusion that physical violence or the threat of physical violence will remain the ultimate means of coercion.[37]

The Problem of Battle Damage Assessment

Theoretically, if you can functionally destroy or sufficiently disrupt command, control, and communications, physical destruction of C3 assets will be unnecessary. Furthermore, if you can sever the head from the arms by isolating the leadership from its armed forces, you may obviate the need to engage the enemy's armed forces in "real" combat at all. Unfortunately, IW battle damage assessment is even less well developed than IW itself. The problem is obvious. We have developed the tools and techniques to assess physical damage quite well, but a "soft kill" is generally indistinguishable from a "miss." The experience with Iraqi power distribution stations is an excellent example. The carbon fiber filaments from the Tomahawk "Kit 2" warheads shorted Iraqi power grid systems so badly, they fused generators, but because the damage was not visible, they were hit again with iron bombs, "just to

make sure."[38] It is very likely that IW experience will be very similar. Even if we achieve OIW successes, they are likely to be followed up with hard target kills.

CONCLUSIONS AND CAVEATS: FEASIBILITY AND DESIRABILITY

Conclusions

Piercing the fog of war has been a goal of military leaders, since the time of Sun Tzu. The capabilities of modern digital technology and communication bring both extraordinary opportunities and dangers. We can see the potential to "read the enemy like an open book." At the same time, we may be able to confound the enemy by destroying or disrupting his own information systems. In so doing, we can increase his friction and thicken the fog of war until it is virtually impenetrable. From this perspective, offensive IW is both feasible and desirable.

The information revolution presents a two-edged sword, however. As our capability is leveraged by information technology, so is our vulnerability to disruption. While the same is true for an enemy, one message should ring loud and clear - defense of our own information systems is even more important than the disruption or destruction of an enemy's. Defensive IW may not seem terribly appealing, but its effects are desirable, and it is not only feasible, it is absolutely essential.

Caveats

We must not overlook the fact that one who is not dependent on a digital information architecture may be relatively invulnerable to offensive information operations. Consequently, there are conceivable situations in which OIW is not particularly feasible. We need to remember that fact, lest we find ourselves expecting IW to accomplish effects against an enemy that simply isn't vulnerable.

While the opportunities for synergy and high payoff are great in offensive information warfare, the penalties for neglecting defensive information warfare are even greater. The United States military leads the world in digitization of information systems, and has achieved this preeminence at great expense. Attention to defense of this capability is imperative, to defend both the capability and the investment made to create the capability. Neglect of IW defense could lead to an information equivalent of Pearl Harbor. No form of warfare is desirable to the one who finds himself on the losing side, experiencing catastrophe.

Finally, we must be careful not to expect too much of this new weapon of warfare. Information warfare will not be the answer to every challenge. Experience has taught us, for example, that strategic bombing does not win wars by itself. It sets the stage, and prepares the battlefield for extraordinary success of ground forces, contributing enormously to synergy. As such, it is an indispensable part of the US military repertoire. But there are limits to the ends that can be accomplished through aerial bombardment. Just as strategic aerial bombardment has become a powerful tool, but not a panacea or end to conventional combat, so information warfare is likely to

become an indispensable tool when used appropriately against an enemy's vulnerability. While we may conclude that information warfare is both feasible, and preferable to "traditional" combat, we must remember the warning of Carl von Clausewitz, against concluding that successful maneuver is the object of battle. It is battle that is the object of maneuver, and bloody combat is the "cash transaction" of war. If we expect IW to entirely replace "old fashioned" combat, we are sure to be painfully disappointed, and shocked by the price of the cash transaction.

ENDNOTES

1. General Gordon E. Sullivan, "Future Vision," Military Review, May-June 1995, 5.

2. General Dennis J. Reimer, "The World's Best Army - America's Army," lecture presented to the U.S. Army War College Class of 1996, August 14, 1995.

3. National Military Strategy of the United States 1995 - A Strategy of Flexible and Selective Engagement, U.S. Government Printing Office, Washington, DC, 4.

4. Alvin and Heidi Toffler, Chapter 8, "The Way We Make Wealth..." War and Anti-War, Warner Books, New York, 1995, 64-72.

5. Ibid, Chapter 9, "Third Wave War" 73-93. This extension of Toffler's previous thesis is the heart this book: information is not only a source of wealth and power, it is by extension a new means of exerting influence, and imposing one's will - a new weapon of war.

6. Dennis K. Miner, "A Curriculum for Strategy in the Information Age: Chaos in a New Era," U.S. Army War College Strategy Research Project, Carlisle Barracks, Pennsylvania, 1995, 18. Miner proposed a "hierarchy of thought process" shaped like a pyramid, with some similar elements. This "Hierarchy of Data, Information/Knowledge" is my own refinement, and differs in that it identifies the processes that produce information from data, knowledge from information, and wisdom from knowledge. My own hierarchy also contends that communication is not just a single layer, but resides between each of the layer. This distinction is important, as it leads to identification of *communication* as a key target for disruption or destruction.

7. Peter Grier, "Information Warfare," Air Force Magazine, March 1995, Vol 78, No. 3, 34.

8. Department of Defense Directive 3600.1, Information Warfare.

9. LtCol Norman B. Hutcherson, USAF, "Command & Control Warfare - Putting Another Tool in the War Fighter's Data Base," Research Report No. AU-ARI-94-1, Air University Press, Maxwell AFB, AL, September 1994, xiii.

10. Battlefield of the Future - 21st Century Warfare Issues, Air War College Studies in National Strategy No.3, "Overview: Information Warfare Issues," Air University Press, Maxwell Air Force Base, Alabama, September 1995, 149-151. The editors identify a problem that continues to impede critical thinking about Information Warfare throughout the US armed forces: an attempt by many to view IW as simply an outgrowth or extension of familiar forms of combat or combat support, such as intelligence or electronic warfare operations. In their introduction to IW in this volume they state: "'Information warfare' is not the same as intelligence operations, although it is clearly related to intelligence. As it is emerging in Defense Department thinking, IW is an attack on the adversary's entire information, command and control, and, indeed, decision-making system."

11. John Arquilla and David Ronfeldt, "Cyberwar is Coming!" Comparative Strategy, Volume 12, No.2, Taylor & Francis, Bristol, Pennsylvania, 1993. I pulled this article up from a WEB site where it was also published (http://www.stl.nps.navy.mil/c4i/cyberwar.html), so the following page numbers refer to the cyber version rather than the Comparative Strategy publication. Page 1.

12. Ibid., 8.

13. Colonel Edward Mann, USAF "Desert Storm - The First Information War," Airpower Journal, Winter 1994, Vol. VIII, No. 4, page 5.

14. David Fulghum, "Secret Carbon Fiber Warheads Blinded Iraqi Air Defenses," Aviation Week and Space Technology, April 27, 1992, Vol 136, No. 17, 18-20.

15. Rick Atkinson, CRUSADE - The Untold Story of the Persian Gulf War, Houghton Mifflin Company, New York, 1993, 18-33.

16. Winn Schwartau, Information Warfare - Chaos on the Electronic Superhighway, Thunder's Mouth Press, New York, 1994. 250-251. Both "ABC Nightline" and U.S. News and World Report carried this story in February 1992. In retrospect, it appears the source of the story was an article in InfoWorld on April 1, 1991, which was, in fact an April Fools joke. Schwartau's point is not that computer viruses are inapplicable in warfare, but that delivering a printer with a virus at the last minute is a very unlikely way to insert such a weapon.

17. Field Manual 100-5, Operations, Headquarters, Department of the Army, June 1993, (CD-ROM edition) Chapter 9, "Fundamentals of the Defense." Clearly, the US Army is deliberate in its attempt to maintain an offensive spirit, and prevent development of a defensive mind set. In the subchapter titled "Purpose of the Defense" it states categorically, "Military forces defend only until they gain sufficient strength to attack." The logic and the motivation are both sound, especially for ground combat operations, but the emphasis may denigrate the importance of successful defense.

18. Alan D. Campen, USAF, "Vulnerability of Information Systems Demands Immediate Attention," National Defense, Nov.95, Vol LXXXI, No. 512, 26.

19. Deborah Russel and G. T. Gangemi, Computer Security Basics, O'Reilly & Associates, Inc., Sebastopol, California, 1991, 55-77. In their chapter titled "Computer System Security and Access Controls," Russell and Gangemi use terms and analogies that would be comfortably familiar to most military personnel, including a "military security model" that groups information by sensitivity into four levels: TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED. The thrust of the chapter, however, is a discussion of four primary methods of providing protection for computer systems: 1) system access controls (who has physical access to the system and permission to use it), 2) data access controls (who has permission to read, write, or modify files), 3) system and security administration (administration, training, and monitoring/enforcing security procedures), and 4) system design.

20. Steve Gilliland, "Nine No-Cost Steps to a Secure LAN", Computer Shopper, November 1995, 635-637. Gilliland is blunt in his assessment of the greatest threat to computer network security: "The biggest threat to your network security system logs on every day, and it's not some remote hacker. It's the workstation operator who has decided that entering a password every day is too much work." Unsecure or trivial passwords are the IW analog to safe combinations and file cabinet keys in desk drawers.

21. Mark Clodfelter, The Limits of Airpower - the American Bombing of North Vietnam, The Free Press, New York, 1989. 2. During the interwar period, the prophets of airpower - Giulio Douhet, Hugh Trenchard, and William "Billy" Mitchell published numerous works advancing the theory that strategic bombing could destroy an enemy's capability to fight, and more- that it would ultimately destroy an enemy's will to fight. Douhet's Command of the Air is considered by many to be the seminal work of the period.

22. Earl H. Tilford Jr., Crosswinds - the Air Force's Setup in Vietnam, Texas A&M University Press, College Station, 1993. 186-188. This particular lament is heard most often in conjunction with the Vietnam War, and Tilford lists it among several "unhealthy myths." The essence of Tilford's thesis is that the leadership of the Air Force and the nation assumed incorrectly that if airpower could prevail in a major war, it could also resolve any smaller conflict. Tilford contends that the use of strategic bombing against a pre-industrial society was largely ineffective.

23. Thomas B. Allen and Norman Polmar, Code Name Downfall, Simon & Schuster, New York, 1995, 259-289. The atomic bomb was a shock, but not universally. General Korechika Anami, the Japanes War Minister, held out for defense of the homeland, to convince the Allies that invasion and occupation would extract a price that the Allies would be unwilling to pay. Anami was adamant, even after the bombing of Hiroshima and Nagasaki, and deadlocked the Cabinet, forcing Premier Suzuki to seek a decision from the Emperor- unheralded in modern times. The authors suggest that the "new and cruel bomb" provided an *excuse* for Hirohito to direct not only the government, but the society to "bear the unbearable" - the surrender he had long-since determined was necessary and inevitable.

24. Tilford, 4.

25. MacIsaac, U.S. Strategic Bombing Survey, Vol I - Overall Report (Europe). 108. This report concludes that the bombing of German cities did not *strengthen* the resolve of the civilian population, and attributes the perseverance of the civilian population to the influence of the police state. Perhaps, but that is still a far cry from destroying the enemy's will to fight, and how does one account for the behavior and attitude of Londoners during the Battle of Britain?

26. Allen and Polmar, 274. Is occupation of a prostrate opponent important? Apparently so, especially to the vanquished. On August 9, 1945, the Japanese Supreme Council for the Direction of the War met to discuss Japan's surrender to the Allies. A majority of the Council demanded the following conditions as term for surrender: the Emperor would remain in place, Japan would not be occupied, war crime trials would not be held, and the Japanese armed forces would disarm themselves. Of these terms, the Allies accepted only the retention of the Emperor. In light of recent experience with Iraq, and its leader's recalcitrance, it is difficult to imagine what Japan might have been like if it had not been occupied.

27. Tom Clancy, Debt of Honor, Berkley Books, New York, 1995.

28. Schwartau, 96-97. Schwartau relates the story of the Bank of New York, when it found itself short $23 billion at the close of business on November 21, 1985. It cost the bank $3.1 million in overnight interest while software engineers found and fixed the software bug responsible. If this sort of disruption can occur by accident, the implications for a determined attack are sobering.

29. Toffler, 3. "Anti-war," as defined be the Tofflers, refers to "actions taken to avoid, avert, or mitigate war" - including small wars undertaken to prevent larger wars. Anti-wars involve the application of military, economic, and *informational* power to reduce the violence associated with change.

30. George J. Stein, "Information War - Cyberwar - Netwar," Battlefield of the Future - 21st Century Warfare Issues, Air War College Studies in National Strategy No.3, Air University Press, Maxwell Air Force Base, Alabama, September 1995, 153-170. Stein, who relies heavily on the article by Arquilla and Ronfeldt, argues convincingly that Information Warfare, or netwar, as he defines the term, only produces chaos and anarchy - hardly a definable war aim or strategic

objective. His premise is that "the end state of netwar may not be bloodless surrender, but total disruption of the targeted society."

31. Campen, 27.

32. John Arquilla, "The Strategic Implications of Information Dominance," Strategic Review, Summer 1994, Vol XXII, No. 3, 24-30. Arquilla points out that air power from World War II to Vietnam generally failed to find and destroy the opponent's center of gravity. He maintains that the results in the Gulf War were different, due to detailed coalition knowledge of Iraq's communications infrastructure. While one may argue over the ability of coalition airpower to find and destroy Iraq's strategic center of gravity, there is little argument that air strikes virtually eliminated Baghdad's ability to command and control Iraq's fielded forces. The limited number of coalition casualties indicates the preparation of the battlefield through the application of airpower at appropriate targets, including informational targets, was indeed effective.

33. Mann, 5.

34. Tom Mangold, and John Penycate, The Tunnels of Cu Chi, Berkley Books, New York, 1986, 125-143. Random House printing, 1985. Problems encountered by US forces in Vietnam by clever enemy use of imitative deception will be familiar to most readers. Communist forces mimicked US radio traffic, directing US artillery and air strikes on US forces. Both the physical and demoralizing effects were predictable. It was an expensive lesson, but it taught US forces once again the value of rigorous attention to radio procedures and good communications security. The experience described by Mangold and Penycate is quite different, but just as applicable. The 25th Infantry Division built its headquarters directly on top of an area that had been extensively prepared by Viet Cong insurgents for years. The tunnel complex was simply unbelievable. Even though the Division secured the perimeter on the surface, costly attacks originating from *within* the base continued with demoralizing persistence. "They were uncovering tunnels for months, if not a year," according to one battalion commander. IW attacks hold the potential for an analogous experience - attacks that appear to originate from within the nation's otherwise secure borders, and are maddeningly difficult to detect or prevent.

35. Schwartau, 363.

36. Stein, 161. George Stein contends that the potential effects of unlimited IW on the infrastructure of a nation may rival those of nuclear warfare. How would a modern, densely populated society cope with no electricity, potable water, communications, transportation, food distribution, or modern medical appliances? Consequently, he contends that opponents will reach a "Mexican standoff" analogous to the deterrence of "Mutual Assured Destruction" in the Cold War. This may in fact prove to be the case between nation-states, but it ignores the emergence and increasing capability of non-state actors.

37. General Gordon R.Sullivan, and Colonel James M. Dubick, "War in the Information Age," Military Review, Volume LXXIV, April 1994, No.4, pages 55 and 62.

38. Atkinson, 38, 116.

BIBLIOGRAPHY

A National Security Strategy Of Engagement and Enlargement, The White House, February 1995.

Allen, Thomas B., and Palmer, Norman, Code Name Downfall, Simon & Schuster, New York, 1995, 259-289.

Arquilla, John, "the Strategic Implications of Information Dominance," Strategic Review, Summer 1994, Vol XXII, No. 3, 24-30.

Arquilla, John, and Ronfeldt, David, "Cyberwar is Coming!" Comparative Strategy, Volume 12, No.2, Taylor & Francis, Bristol, Pennsylvania, 1993.

Atkinson, Rick, CRUSADE - The Untold Story of the Persian Gulf War, Houghton Mifflin Company, New York, 1993.

Battlefield of the Future - 21st Century Warfare Issues, Air War College Studies in National Strategy No.3," Overview: Information Warfare Issues," Air University Press, Maxwell Air Force Base, Alabama, September 1995, 149-151.

Campen, Alan D., USAF, "Vulnerability of Information Systems Demands Immediate Attention," National Defense, Nov.95, Vol LXXXI, No. 512, 26-27.

Clancy, Tom, Debt of Honor, Berkley Books, New York, 1995.

Clausewitz, Carl Von, On War, edited and translated by Michael Howard and Peter Paret, Princeton University Press, Princeton, New Jersey, 1976.

Clodfelter, Mark, The Limits of Airpower - the American Bombing of North Vietnam, The Free Press, New York, 1989.

Department of Defense Directive 3600.1, Information Warfare.

"E-8C Joint STARS," sales/promotion brochure, published by Grumman Melbourne Systems of Grumman Northrop, Melbourne, Florida.

Fulghum, David, "Secret Carbon Fiber Warheads Blinded Iraqi Air Defenses," Aviation Week and Space Technology, April 27, 1992, Vol 136, No. 17, 18-20.

Steve Gilliland, "Nine Low Cost Steps to a Secure LAN", Computer Shopper, November 1995, 635-637.

Grier, Peter, "Information Warfare," Air Force Magazine, March 1995, Vol 78, No. 3, page 34.

Howard, Michael, Clausewitz, Oxford University Press, Oxford, 1983.

Hutcherson, LtCol Norman B., USAF, "Command & Control Warfare - Putting Another Tool in the War Fighter's Data Base," Research Report No. AU-ARI-94-1, Air University Press, Maxwell AFB, AL, September 1994.

"Information Warfare - Legal Regulatory, Policy, and Organizational Considerations for Assurance," A Research Report for the Chief, Information Warfare Division (J6K), Command, Control, Communications and Computer Systems Directorate, Joint Staff, The Pentagon, prepared by Science Applications International Corporation (SAIC), 4 July 1995.

Mangold, Tom, and Penycate, John, The Tunnels of Cu Chi, Berkley Books, New York, 1986. Random House printing, 1985.

Mann, Colonel Edward, USAF "Desert Storm - The First Information War," Airpower Journal, Winter 1994, Vol. VIII, No. 4. Pages 4-13.

Miner, Dennis K., "A Curriculum for Strategy in the Information Age: Chaos in a New Era," U.S. Army War College Strategy Research Project, Carlisle Barracks, Pennsylvania, 1995.

National Military Strategy of the United States 1995 - A Strategy of Flexible and Selective Engagement, U.S. Government Printing Office, Washington, DC.

Reimer, General Dennis J., "The World's Best Army - America's Army," lecture presented to the U.S. Army War College Class of 1996, August 14, 1995.

Russel, Deborah, and Gangemi, G. T., Computer Security Basics, O'Reilly & Associates, Inc., Sebastopol, California, 1991.

Schwartau, Winn, Information Warfare - Chaos on the Electronic Superhighway, Thunder's Mouth Press, New York, 1994.

Stein, George J., "Information War - Cyberwar - Netwar," Battlefield of the Future - 21st Century Warfare Issues, Air War College Studies in National Strategy No.3, Air University Press, Maxwell Air Force Base, Alabama, September 1995, 153-170.

Sullivan, General Gordon E., "Future Vision," Military Review, May-June 1995, pages 4-14.

Sullivan, General Gordon R., and Dubick, Colonel James M., "War in the Information Age," Military Review, Volume LXXIV, April 1994, No.4, pages 46-62.

Sweetman, Lieutenant-Colonel J. P., "New Thinking In the U.S. Army: The Louisiana Maneuvers, Battle Laboratories, and The Third Wave Army," Canadian Defence Quarterly, Vol. 124, No. 1, September 1994.

"The Softwar Revolution, A Survey of Defence Technology," The Economist, June 10th 1995. Bibliography on the Internet at http://www.earthlink.net/~the-economist/

Tilford, Earl H. Jr., Crosswinds - the Air Force's Setup in Vietnam, Texas A&M University Press, College Station, 1993.

Toffler, Alvin, The Third Wave, Morrow, New York, 1980.

Toffler, Alvin and Heidi, War and Anti-War, Warner Books, New York, 1995.

U. S. Army Field Manual 100-5, Operations, Headquarters, Department of the Army, June 1993. (CD-ROM Multimedia Edition)

U.S. Strategic Bombing Survey, Vol I - Overall Report (Europe)